

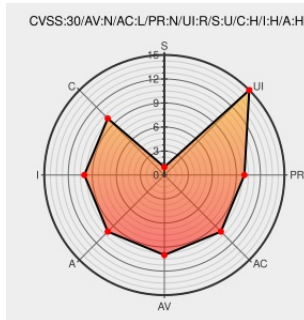


# CVE-2014-0158

Published on: 04/10/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:55 PM UTC

## CVE-2014-0158

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Opensuse](#) from [Opensuse](#) contain the following vulnerability:

Heap-based buffer overflow in the JPEG2000 image tile decoder in OpenJPEG before 1.5.2 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted file because of incorrect j2k\_decode, j2k\_read\_eoc, and tcd\_decode\_tile interaction, a related issue to CVE-2013-6045. NOTE:

this is not a duplicate of CVE-2013-1447, because the scope of CVE-2013-1447 was specifically defined in <http://openwall.com/lists/oss-security/2013/12/04/6> as only "null pointer dereferences, division by zero, and anything that would just fit as DoS."

CVE-2014-0158 has been assigned by [secalert@redhat.com](mailto:secalert@redhat.com) to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.8 - HIGH**

| Attack Vector    | Attack Complexity      | Privileges Required | User Interaction    |
|------------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b>   | <b>LOW</b>             | <b>NONE</b>         | <b>REQUIRED</b>     |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>HIGH</b>            | <b>HIGH</b>         | <b>HIGH</b>         |

CVSS2 Score: **6.8 - MEDIUM**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>MEDIUM</b>     | <b>NONE</b>         |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>PARTIAL</b>         | <b>PARTIAL</b>    | <b>PARTIAL</b>      |

## CVE References

| Description | Tags | Link |
|-------------|------|------|
|-------------|------|------|

|                                                                                                        |                                                                                                                                            |                                                                                     |
|--------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| Bug 1082925 – openjpeg: Heap-based buffer overflow in JPEG2000 image tile decoder                      | <a href="#">Issue Tracking</a><br><a href="#">Third Party Advisory</a><br><a href="#">bugzilla.redhat.com</a><br><a href="#">text/html</a> | <a href="#">MISC</a><br><a href="#">bugzilla.redhat.com/show_bug.cgi?id=1082925</a> |
| Bug 871412 – VUL-0: CVE-2014-0158: openjpeg: heap-based buffer overflow in JPEG2000 image tile decoder | <a href="#">Issue Tracking</a><br><a href="#">Third Party Advisory</a><br><a href="#">bugzilla.suse.com</a><br><a href="#">text/html</a>   | <a href="#">MISC</a><br><a href="#">bugzilla.suse.com/show_bug.cgi?id=871412</a>    |

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](mailto:comment@cve.report).

There are currently no QIDs associated with this CVE

| Known Affected Configurations (CPE V2.3) |                           |                          |         |        |         |          |
|------------------------------------------|---------------------------|--------------------------|---------|--------|---------|----------|
| Type                                     | Vendor                    | Product                  | Version | Update | Edition | Language |
| Operating System                         | <a href="#">Opensuse</a>  | <a href="#">Opensuse</a> | 12.3    | All    | All     | All      |
| Operating System                         | <a href="#">Opensuse</a>  | <a href="#">Opensuse</a> | 13.1    | All    | All     | All      |
| Operating System                         | <a href="#">Opensuse</a>  | <a href="#">Opensuse</a> | 12.3    | All    | All     | All      |
| Operating System                         | <a href="#">Opensuse</a>  | <a href="#">Opensuse</a> | 13.1    | All    | All     | All      |
| Application                              | <a href="#">Uclouvain</a> | <a href="#">Openjpeg</a> | All     | All    | All     | All      |
| Application                              | <a href="#">Uclouvain</a> | <a href="#">Openjpeg</a> | All     | All    | All     | All      |
| cpe:2.3:o:opensuse:opensuse:12.3:*****:  |                           |                          |         |        |         |          |
| cpe:2.3:o:opensuse:opensuse:13.1:*****:  |                           |                          |         |        |         |          |
| cpe:2.3:o:opensuse:opensuse:12.3:*****:  |                           |                          |         |        |         |          |
| cpe:2.3:o:opensuse:opensuse:13.1:*****:  |                           |                          |         |        |         |          |
| cpe:2.3:a:uclouvain:openjpeg:*****:      |                           |                          |         |        |         |          |
| cpe:2.3:a:uclouvain:openjpeg:*****:      |                           |                          |         |        |         |          |

No vendor comments have been submitted for this CVE

completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](#)